

Abstract

A software application installable on a personal computer protects the computer's primary data files from being accessed by malicious code (e.g., viruses, worms and trojans) imported from an external data source, such as the Internet. A master file serves as the image from which all other software code and functions are derived. Activation of the master image file establishes a secondary operating environment (isolation bubble) in which a secondary operating system including a browser and any other desired applications are installed and run. Access permissions for communications between the computer at large (primary operating system) and the secondary operating system to prevent any access to the files on the primary operating system from any operations originating from the secondary operation system. Activation of the secondary operating system is required before any connection to the Internet (or other external data source) is enabled.